California Blockchain Working Group

Cybersecurity, Risk & Privacy

Jason Albert, Workday
Arshad Noor, StrongKey

Questions to be Addressed

1. What considerations should public or private organizations undertake regarding the security requirements of a proposed implementation of blockchain?

2. Which stakeholders should be involved in such discussions? Should different blockchain systems be associated with different application contexts?

3. What components of blockchain should be highlighted? Can the immutability of blockchain architecture be reconciled with requirements of emerging privacy policies, such as GDPR in the EU and CCPA in California? How should these components be incorporated into a decision-making and assessment process to determine its appropriateness for any use case?

4. How can we ensure that we forge an adaptive path forward for blockchain implementation in California, one that is neither too permissive nor too constrained? Consider implications beyond this legislation.

Security Considerations - 1

1.What considerations should public or private organizations undertake regarding the security requirements of a proposed implementation of blockchain?

a)Security must play a primary role and leverage ***disruptive defenses***

b)Blockchain developers must be certified to write secure blockchain applications

c)State must use only *permissioned* blockchains for an experimental period

d)Consensus protocol must be robust to ensure *distributed ledger* is not compromised

e)Risk of social-engineering attacks and fraud must be mitigated

f)Risk of *smart contracts* must be mitigated – eliminate use during experimental period

Security Considerations - 2

Disruptive Defenses**:** Uncommon defenses, based on industry-standards, that raises application security to new – and higher – levels

a)Eliminating *shared-secret* authentication schemes with *public-key cryptography* using, in general, cryptographic hardware[#]

b)Ensuring the provenance of the transaction before it enters the blockchain

c)Preserving the confidentiality of sensitive information *within*[*] and outside the blockchain

d)Preserving the integrity of transaction data even when outside the blockchain

e)In general, using cryptographic hardware where cryptographic keys are used within the application[#]

f)Application access to cryptographic services remains within a *secure zone*[**]

[*] See Question #3 for recommendations

[**] https://www.ibm.com/developerworks/cloud/library/cl-regcloud/

[#] Agency-specific BCWGs will guide specific risk-mitigation measures. See Question #4 for recommendations

Stakeholders; Different Blockchains?

2.Which stakeholders should be involved in such discussions?

- Business representatives
- Government representatives of existing systems-of-record
- Independent legal and privacy advisers
- Experienced regulators from sectors such as construction, finance and utilities
- Application and cryptography security experts – not network security experts
- Representatives of public affected by blockchain system

Should different blockchain systems be associated with different application contexts?

- Yes

Immutability and Privacy in Blockchains

3.What components of blockchain should be highlighted? Can the immutability of blockchain architecture be reconciled with requirements of emerging privacy policies, such as GDPR in the EU and CCPA in California? How should these components be incorporated into a decision-making and assessment process to determine its appropriateness for any use case?

- Neither extreme is desirable; regulation must balance the need for individual privacy with transparency to serve public good
- Applications must be designed to ensure both, but policy must prescribe what takes precedence in the event of a conflict – although currently, it is not clear if any conflict may/need arise
- While data on a blockchain cannot be deleted, several technical solutions make it possible to achieve the same result: i) *Deletion of private-key*; ii) *Deletion of underlying data*; iii) *Encryption of payload*; iv) *Tokenization*; ...

Adaptive Path Forward

4.How can we ensure that we forge an adaptive path forward for blockchain implementation in California, one that is neither too permissive nor too constrained? Consider implications beyond this legislation.

- Blockchain is a paradigm shift with life-changing consequences. Guiding principle should be to ensure no new harm befalls those affected by the change
- Establish permanent BCWG to guide State on path forward for public-sector blockchains, consisting of:
  - Business representatives
  - Government representatives of existing systems-of-record
  - Independent legal and privacy advisers
  - Experienced regulators from sectors such as construction, finance and utilities
  - Application and cryptography security experts – not network security experts
  - Representatives of public affected by blockchain system